UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,072	03/09/2005	Kazuo Omori	SONYJP 3.3-326	2827

530 7590 04/29/2008

LERNER, DAVID, LITTENBERG,
KRUMHOLZ & MENTLIK
600 SOUTH AVENUE WEST
WESTFIELD, NJ 07090

EXAMINER	
PACHURA, REBECCA L	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
04/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/527,072	OMORI ET AL.	
	Examiner	Art Unit	
	Rebecca L. Pachura	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 March 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 March 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *04/09/2008, 01/17/2008, 03/09/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-20 are presented for examination.**

The claims and only the claims form the metes and bounds of the invention. "Office personnel are to give claims their broadest reasonable interpretation in light of the supporting disclosure. In re Morris, 127 F.3d 1048, 1054-55, 44 USPQ2d 1023, 1027-28 (Fed. Cir. 1997). Limitations appearing in the specification but not recited in the claim are not read into the claim. In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-551 (CCPA 1969)" (MPEP p 2100-8, c 2, l 45-48; p 2100-9, c 1, l 1-4). The Examiner has full latitude to interpret each claim in the broadest reasonable sense. The Examiner will reference prior art using terminology familiar to one of ordinary skill in the art. Such an approach is broad in concept and can be either explicit or implicit in meaning.

Information Disclosure Statement

2. The information disclosure statements (IDS) submitted on 04/09/2008 and 03/09/2005 are in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statements are being considered by the examiner. The information disclosure statement filed 01/17/2008 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because the applicant did not submit any translations of the sited art. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

Preliminary Amendment

3. The preliminary amendment to the claims submitted on 10/24/2006 is duly noted. The preliminary amendment to the disclosure submitted on 10/24/2006 is duly noted. The new abstract submitted on 10/24/2006 is duly noted.

Priority

4. The claim for foreign priority from application #2002-273903 from Japan filed on September 9, 2002 is duly noted.

Specification

5. The disclosure is objected to because of the following informalities: The term AP is used throughout the disclosure without any explanation for what it means. Appropriate correction is required.

The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.

Claim Objections

6. Claims 4-10, 14-18, and 20 are objected to because of the following informalities: claims 4-10 and 14-18, line 1 state *"A data processing method"* they should state *"The data processing method"*; claim 20, line 7 states *"second authentication data"* it should state *"second authentication use data"*. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. **Claims 4, 6, 7, 13, 15, 19, and 20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.**

Claims 4, 6, and 15 recite the limitation *"the functions"* and *"the data"* in lines 2, 3, and/or 4. There is insufficient antecedent basis for this limitation in the claim.

Claim 7 recites the limitation *"the plurality of data modules"* in line 2. There is insufficient antecedent basis for this limitation in the claim.

Claims 13 and 19 recite the limitation *"the results"* in lines 10 or 11. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. **Claims 2, 12, 19, and 20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.** As to independent claim 2 and 19, in the preamble the applicant states that it is a system claim. In a system claim there must be a hardware component such as a processor or memory that the software modules are stored in or run on. As to the independent claims 12 and 20, the preamble recites *"A program for causing a*

data processing system" a program must be embodied in something, such as a storage medium, in order to be statutory subject matter. As well as in a system claim there must be a hardware component such as a processor or memory that the software modules are stored in or run on. In view of the below sited MPEP section the claim is non-statutory because it is functional descriptive material per se.

> **MPEP 2106.01 [R-5]**
> Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." In this context, "functional descriptive material" consists of data structures and computer programs which impart functionality when employed as a computer component. (The definition of "data structure" is "a physical or logical relationship among data elements, designed to support specific data manipulation functions." The New IEEE Standard Dictionary of Electrical and Electronics Terms 308 (5th ed. 1993).)
> Both types of "descriptive material" are nonstatutory when claimed as descriptive material per se, 33 F.3d at 1360, 31 USPQ2d at 1759.

Claim Rejections - 35 USC § 102

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

9. **Claims 1-16, 19, and 20 are rejected under 35 U.S.C. 102(b) as being anticipated by US 6240517 (Nishioka).**

As to claim 1, Nishioka discloses (currently amended) a data processing method performed by ~~a~~ means to be authenticated and authenticating means, the means to be authenticated ~~for~~ holding first authentication use data generated by encryption using key data and ~~an~~ the authenticating means ~~for~~ holding the key data, the method comprising:

~~a first step by which the means to be authenticated provides~~ providing key designation data designating the key data from the means to be authenticated to the authenticating means (Nishioka column 11, lines 37-59);

~~a second step by which the authenticating means performs~~ performing encryption at the authenticating means using the ~~key data~~ designated ~~by the~~ key ~~designation~~ data ~~received at the first step~~ to generate second authentication use data (Nishioka column 11, lines 60-64);

~~a third step by which the means to be authenticated uses~~ comparing the first authentication use data ~~for authentication and uses~~ with the second authentication use data ~~for authentication~~; and (Nishioka column 11, lines 64-67)

~~a fourth step by which the authenticating means executes~~ executing processing related to the key data in the authenticating means when the ~~authentication at the third step decides~~ comparison determines that the first authentication use data and the second authentication use data are the same (Nishioka column 11, line 67 and column 12, lines 1-12).

As to claim 2, Nishioka discloses (currently amended) a data processing system comprising:

~~a~~ means to be authenticated for holding first authentication use data generated by encryption using key data; and (Nishioka Figure 16, #330)

~~an~~ authenticating means for holding the key data (Nishioka Figure 16, #530),

wherein the means to be authenticated provides key designation data designating the key data to the authenticating means (Nishioka column 11, lines 37-59),

the authenticating means performs encryption using the ~~key data~~ designated ~~by the~~ key ~~designation~~ data ~~received from the means to be authenticated~~ to generate second authentication use data (Nishioka column 11, lines 60-64),

the means to be authenticated uses the first authentication use data for authentication and the authenticating means uses the second authentication use data for authentication, and (Nishioka column 11, lines 42-54 and lines 60-64)

the authenticating means executes the processing related to the key data when the ~~authentication decides that the~~ first authentication use data and the second authentication use data are the same (Nishioka column 11, line 67 and column 12, lines 1-12).

As to claim 3, Nishioka discloses (currently amended) a data processing method ~~where~~ in which an authenticating means holding predetermined key data performs an authentication process together with a means to be authenticated holding first authentication use data generated by encryption using the key data, the method comprising:

~~a first step of~~ receiving key designation data for designating the key data from the means to be authenticated (Nishioka column 11, lines 60-64);

~~a second step of~~ generating second authentication use data by encryption using the ~~key data~~ designated ~~by the~~ key ~~designation~~ data ~~received at the first step for encryption to generate second authentication use data~~ (Nishioka column 11, lines 60-64: authenticator generation function);

~~a third step of using~~ comparing the second authentication use data ~~generated at the second step for authentication~~ with ~~the means to be authenticated using~~ the first authentication use data ~~for authentication~~ (Nishioka column 11, lines 64-67);

and ~~a fourth step of~~ executing processing related to the key data when the ~~authentication at the third step decides~~ comparison determines that the first authentication use data and the

second authentication use data are the same (Nishioka column 11, line 67 and column 12, lines 1-12).

As to claim 4, Nishioka discloses (currently amended) a data processing method as set forth in claim 3, ~~further comprising, in the fourth step,~~ wherein the executing step includes executing the functions of the authenticating means authorized to the means to be authenticated related to the key data or accessing the data held by the authenticating means (Nishioka column 10, lines 10-30).

As to claim 5, Nishioka discloses (currently amended) A data processing method as set forth in claim 3, ~~further comprising, when the authentication use data is generated by~~ wherein the generating step includes generating the second authentication use date using a plurality of different key data, ~~in the fourth step,~~ and the executing step includes executing a plurality of processings related to the plurality of different key data (Nishioka Figure 16, column 11, lines 60-67, and column 12, lines 1-12).

As to claim 6, Nishioka discloses (currently amended) a data processing method as set forth in claim 5, ~~further comprising, in the fourth step,~~ wherein the executing step includes executing a plurality of processings including the functions of the authenticating means and accessing ~~to~~ the data held by the authenticating means relating to the plurality of different key data (Nishioka Figure 16, column 11, lines 60-67, and column 12, lines 1-12).

As to claim 7, Nishioka discloses (currently amended) a data processing method as set forth in claim 3, ~~further comprising, in the fourth step,~~ wherein the executing step includes accessing the plurality of data modules related to single key data when the authenticating means

holds a plurality of data modules as data (Nishioka Figure 16: the switching unit 500 accesses the first and second authentication data (plurality of data modules) in comparator 540).

As to claim 8, Nishioka discloses (currently amended) a data processing method as set forth in claim 3, ~~further comprising, in the first step,~~ wherein the receiving step includes receiving the key designation data read by a device of the means to be authenticated from an integrated circuit holding the first authentication use data and the key designation data (Nishioka column 11, lines 37-54).

As to claim 9, Nishioka discloses (currently amended) a data processing method as set forth in claim 3, wherein the first authentication use data is data generated by encrypting predetermined data ~~by~~ using the key data (Nishioka column 11, lines 47-54).

As to claim 10, Nishioka discloses (currently amended) a data processing method as set forth in claim 9, wherein the first authentication use data is data generated by encrypting data obtained by encrypting the predetermined data ~~by~~ using the key data by further using tamper-proofing key data managed by the ~~management side~~ means to be authenticated (Nishioka column 13, lines 20-67 and column 14, lines 1-51: the further tamper-proofing is enabled in the third embodiment).

As to claim 11, Nishioka discloses (currently amended) a data processing system holding predetermined key data for use in an authentication process with a means to be authenticated holding first authentication use data generated by encryption using the ~~predetermined~~ key data ~~and holding the key data,~~ the data processing system comprising:

~~an~~ inputting means for inputting key designation data for designating the key data from the means to be authenticated (Nishioka column 11, lines 37-46);

~~an~~ authenticating means for generating second authentication use data by encryption using the ~~key data~~ designated ~~by the~~ key ~~designation~~ data ~~received by the inputting means for encryption to generate second authentication use data~~ and ~~using~~ for comparing the second authentication use data ~~for authentication~~ with the ~~means to be authenticated using the~~ first authentication use data ~~for authentication~~; and (Nishioka column 11, lines 60-67: authenticator generation function)

~~a~~ controlling means for executing processing related to the key data when the ~~authentication~~ comparison by the authenticating means ~~decides~~ determines that the first authentication use data and the second authentication use data are the same (Nishioka column 11, line 67 and column 12, lines 1-12).

As to claim 12, Nishioka discloses (currently amended) a program for causing ~~to be executed by~~ a data processing system holding predetermined key data to execute an ~~for~~ authentication process with a means to be authenticated holding first authentication use data generated by encryption using the ~~predetermined~~ key data ~~and holding the predetermined key data~~, the authentication process comprising (Nishioka column 4, lines 21-40):

~~a first routine of~~ receiving key designation data for designating the key data from the means to be authenticated (Nishioka column 11, lines 60-64);

~~a second routine of~~ generating second authentication use data by encryption using the ~~key data~~ designated ~~by the~~ key ~~designation~~ data ~~received by the first routine to generate second authentication use data~~ (Nishioka column 11, lines 60-64: authenticator generation function);

~~a third routine of using~~ comparing the second authentication use data ~~generated by the second routine for authentication~~ with ~~the means to be authenticated using~~ the first authentication use data ~~for authentication~~; and (Nishioka column 11, lines 64-67)

~~a fourth routine of~~ executing processing related to the key data when the ~~authentication in the third routine decides~~ comparison determines that the first authentication use data and the second authentication use data are the same (Nishioka column 11, line 67 and column 12, lines 1-12).

As to claim 13, Nishioka discloses (currently amended) a data processing method performed by a means to be authenticated, ~~when an authenticating means holding key data uses key data designated from~~ the means to be authenticated holding ~~the~~ first authentication use data ~~for~~ generated by encryption using key data ~~to generate second authentication use data, uses the second authentication use data for authentication with the means to be authenticated, and performs processing related to the key data conditional on the authentication confirming that the first authentication use data and the second authentication use data are the same,~~ the method comprising:

~~a first step of~~ providing key designation data ~~for~~ designating the key data used ~~when~~ to generating the first authentication use data ~~based on the predetermined generation method~~ to ~~the~~ authenticating means the authenticating means using the designated key data to generate second authentication use data (Nishioka column 11, lines 55-59);

~~a second step of~~ using the first authentication use data ~~for~~ in an authentication process in which ~~with~~ the authenticating means uses the second authentication use data; and (Nishioka column 11, lines 60-64 and Figure 16)

~~a third step of making~~ causing the authenticating means ~~perform~~ to execute processing related to the key data based on the results of the authentication ~~at the second step~~ process (Nishioka column 11, lines 64-67 and column 12, lines 1-12).

As to claim 14, Nishioka discloses (original) a data processing method as set forth in claim 13, wherein the means to be authenticated reads and holds the first authentication use data and the key designation data from a predetermined integrated circuit (Nishioka column 11, lines 37-54).

As to claim 15, Nishioka discloses (currently amended) a data processing method as set forth in claim 13, ~~further comprising, in the third step, making~~ wherein the causing step includes causing the authenticating means to execute the functions of the authenticating means authorized to the means to be authenticated related to the key data or accessing the data held by the authenticating means (Nishioka column 10, lines 10-30).

As to claim 16, Nishioka discloses (currently amended) a data processing method as set forth in claim 13, wherein ~~further comprising, when defining a group comprising~~

the authenticating means includes a plurality of authenticating means (Nishioka Figure 18),

~~in the first step,~~ the providing step includes collectively providing the key designation data to the ~~group~~ plurality of authenticating means, and (Nishioka Figure 18),

~~in the third step,~~ the causing step includes collectively ~~making~~ causing the ~~group~~ plurality of authenticating means to perform the processings related to the key data (Nishioka column 12, lines 15-67, column 13, lines 1-19, and Figure 18).

As to claim 19, Nishioka discloses (currently amended) a data processing system ~~forming a means to be authenticated when an authenticating means holding key data uses key data designated from the means to be authenticated~~ holding ~~the~~ first authentication use data ~~for~~ generated by encryption using key data, the first authentication use data being for use in an authentication process with an authenticating means ~~to generate second authentication use data, uses the second authentication use data for authentication with the means to be authenticated, and performs processing related to the key data conditional on the authentication confirming that the first authentication use data and the second authentication use data are the same,~~ the data processing system comprising:

~~a first~~ means for providing key designation data for designating the key data used ~~when~~ to generat~~ing~~e the first authentication use data ~~based on the predetermined generation method~~ to the authenticating means, the authenticating means using the designated key data to generate second authentication use data (Nishioka column 11, lines 37-64);

~~a second~~ means for using the first authentication use data ~~for~~ in an authentication process ~~with~~ in which the authenticating means uses the second authentication use data; and (Nishioka column 11, lines 64-67)

~~a third~~ means for ~~making~~ causing the authenticating means ~~perform~~ to execute processing related to the key data based on the results of the authentication ~~of the second means~~ process (Nishioka column 11, line 67 and column 12, lines 1-12).

As to claim 20, Nishioka discloses (currently amended) a program for causing ~~to be executed by~~ a data processing system ~~forming a means to be authenticated when an authenticating means holding key data uses key data designated from the means to be~~

~~authenticated~~ holding ~~the~~ first authentication use data ~~for~~ generated by encryption ~~to generate second authentication use data, uses the second authentication use data for authentication with the means to be authenticated, and performs processing related to the key data conditional on the authentication confirming that the first authentication use data and the second authentication use data are the same~~ using key data to execute an authentication process with authenticating means, comprising (Nishioka column 9, lines 25-49):

~~a first routine of~~ providing key designation data for designating the key data used ~~when~~ to generating~~e~~ the first authentication use data ~~based on the predetermined generation method~~ to the authenticating means, the authenticating means using the designated key data to generate second authentication data (Nishioka column 11, lines 37-64);

~~a second routine of~~ using the first authentication use data ~~for authentication~~ in a comparison with the ~~authenticating means~~ second authentication use data; and (Nishioka column 11, lines 64-67)

~~a third routine of making~~ causing the authenticating means ~~perform~~ to execute processing related to the key data based on the results of the ~~authentication of the second means~~ comparison (Nishioka column 11, line 67 and column 12, lines 1-12).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. **Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over US 6240517 (Nishioka) in view of US 5272754 (Boerbert).**

As to claim 17, Nishioka discloses (currently amended) a data processing method as set forth in claim 13. Nishioka fails to teach further comprising ~~a fourth step of~~ providing a screen displaying an image corresponding to the authenticating means for performing the processing by using a plurality of different patterns in accordance with ~~the~~ an operation state of the authenticating means.

However, Boerbert discloses further comprising ~~a fourth step of~~ providing a screen displaying an image corresponding to the authenticating means for performing the processing by using a plurality of different patterns in accordance with ~~the~~ an operation state of the authenticating means (Boerbert column 5, lines 12-26).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Nishioka and Boerbert because Nishioka discloses a PC, which controls the switching unit (authenticating means), with a display (Nishioka column 8, lines 1-5 and Figure 12) it would be logical that it would display the operation state of the authenticating means such as in Boerbert for diagnostics, for finding out which units are on, for confirming whether or not a means to be authenticated is authentic, etc. (Boerbert column 5, lines 12-26).

As to claim 18, Nishioka discloses (currently amended) a data processing method as set forth in claim 17. Nishioka fails to teach ~~further comprising, in the fourth step,~~ wherein the screen providing step includes providing a screen displaying an image corresponding to the authenticating means by a pattern enabling ~~identification~~ determination of whether ~~or not~~ the

authenticating means ~~already~~ has confirmed the ~~legitimacy~~ authenticity of the means to be authenticated by the authentication ~~in the second step~~ process.

However, Boerbert discloses ~~further comprising, in the fourth step,~~ wherein the screen providing step includes providing a screen displaying an image corresponding to the authenticating means by a pattern enabling ~~identification~~ determination of whether ~~or not~~ the authenticating means ~~already~~ has confirmed the ~~legitimacy~~ authenticity of the means to be authenticated by the authentication ~~in the second step~~ process (Boerbert column 5, lines 12-26).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Nishioka and Boerbert because Nishioka discloses a PC, which controls the switching unit (authenticating means), with a display (Nishioka column 8, lines 1-5 and Figure 12) it would be logical that it would display the operation state (the authenticity of the means to be authenticated) of the authenticating means such as in Boerbert for confirming whether or not a means to be authenticated is authentic, etc. (Boerbert column 5, lines 12-26).

Prior Art

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. US 5288978 is pertinent because it teaches… A mutual authentication system authenticates a first electronic device and a second electronic device by transmitting authentication data between the first and second electronic devices. In this system, the second electronic device transmits a first authentication data to the first electronic device. In the first electronic device, the legitimacy of the second electronic device is determined based on the first authentication data transmitted from the second electronic device. The first electronic device also

transmits a second authentication data, which is used for determining the legitimacy of the first electronic device, to the second electronic device. When the second electronic device is not determined to be legitimate by the first electronic device, the first electronic device does not transmit the second authentication data to the second electronic device. EP 827120 is pertinent because it teaches… Known authentication system for mutual authentication of smart-card terminal/network and smart card has comparison device that compares at least section of second signal originating from second device with at least section of definition signal stored in first memory device. US 20010019614 is pertinent because it teaches… The key database (44) is isolated from the information database (62). The security domain (22) includes a system key manager (84) operable to generate system keys with system key common names and an encryption key manager (24) operable to generate encryption keys having encryption key identifications. The key managers (24, 84) operate on a key server (40), which is mirrored by a secondary key server (42). A general security manager (82) also operates on the key server (40) to control access to the security domain… US 20020126850 is pertinent because it teaches… key management system includes secured data stored on a first system secured by a control key stored securely on a key server. The secured data is secured against attacks such as unauthorized use, modification or access, where authorization to access the secured data is determined by knowledge of an access private key of an access key pair. When an authorized user is to access the secured data, the first system generates a request to the key server, signed with the access private key, wherein the request is for a decryption control key and the request includes a one-time public key of a key pair generated by the first system for the request. The first system can decrypt the decryption control key from the response, using a one-time private key. The first

system can then decrypt the secured data with the decryption control key remaining secured in transport. US 6915434 is pertinent because it teaches… A storage apparatus includes a key management unit for managing an individual key unique to the apparatus and a common key shared with other storage apparatuses, and an encryption unit for performing an encrypting process or verifying data for performing the encrypting process on electronic data stored in the apparatus to which the unit belongs using the individual key, and performing the encrypting process or verifying the data on the electronic data transmitted to or received from another apparatus using the common key. Thus, the apparatus communicates data using an applicable common key in a local environment and a global environment, appropriately manages a key in each environment, and guarantees the security of the electronic data.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Rebecca L. Pachura whose telephone number is (571) 270-3402. The examiner can normally be reached on Monday-Thursday 7:30 am-6:00 pm EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Rebecca L Pachura/
Examiner, Art Unit 2136

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136